A Generalization of Gaussian Sums to Vector Spaces over Finite Fields

Priscilla S. Bremser
Department of Mathematics and Computer Science
Middlebury College
Middlebury, Vermont 05753

Submitted by Hans Schneider

ABSTRACT

Let X be a vector space of dimension n over a finite field $\mathbf{F}_q$ of characteristic $p \neq 2$. We define $L(X)$ to be the set of maps from X to the field of complex numbers; $L(X)$ forms a complex vector space. To each nonsingular linear transformation α of X we associate a linear transformation $\alpha^{\#}$ of $L(X)$. In the case where $n = 1$, f is a multiplicative character χ of F_q, and α is the identity transformation, we have $\alpha^{\#} f(\xi) = q^{-1/2} G(\chi, \psi_\xi)$, where $G(\chi, \psi_\xi)$ is a Gaussian sum for F_q. In this paper we investigate the properties of $\alpha^{\#}$ and show how its eigenvalues can be computed.

1. INTRODUCTION

Let F_q be the finite field with q elements, $q = p^s$ (p prime), and assume $p \neq 2$. For $X = (F_q)^n$, let $L(X)$ be the set of maps f from X to $\mathbf{C}$, the field of complex numbers. The q^n characteristic functions f_ξ, $\xi \in X$, where $f_\xi(x) = \delta_{\xi x}$, form a basis of $L(X)$ as a vector space over $\mathbf{C}$. Let

$$\psi : F_q \to \mathbf{C}$$

be the additive character with

$$\psi(a) = e^{2\pi i \operatorname{tr}(a)/p},$$

52 Vanderbilt Ave., New York, NY 10017 0024-3795/86/$3.50

where $\mathrm{tr}(a)$ is the trace of a in F_p. For $x=(x_1,\ldots,x_n)$ and $y=(y_1,\ldots,y_n)\in X$ let $x\cdot y=x_1y_1+\cdots+x_ny_n\in F_q$.

DEFINITION 1.1. For each $\xi\in X$, define $\psi_\xi: X\to C$ by $\psi_\xi(x)=\psi(\xi\cdot x)$.

As $\psi_\xi(x+y)=\psi_\xi(x)\psi_\xi(y)$, ψ_ξ is a character on the additive group of X, and since the ψ_ξ are distinct, they represent all characters of X.

PROPOSITION 1.2. *$\{\psi_\xi:\xi\in X\}$ is an orthogonal basis for $L(X)$.*

Proof. This follows from the orthogonality relations for characters; see for example [6, p. 189]. ■

We now use the basis $(\psi_\xi\}$ to define a family of linear transformations on $L(X)$.

DEFINITION 1.3. If α is a nonsingular linear transformation of X, define $\alpha^{\#}: L(X)\to L(X)$ by

$$(\alpha^{\#}f)(\xi)=q^{-n/2}\sum_{x\in X}f(x)\psi_\xi(\alpha x).$$

Let χ be a multiplicative character of F_q, and ψ_ξ an additive character. Let $G(\chi,\psi_\xi)$ denote the resulting Gaussian sum; that is, $G(\chi,\psi_\xi)=\sum_{x\in F_q}\chi(x)\psi_\xi(x)$. For $n=1$, $f=\chi$, and α the identity transformation, $(\alpha^{\#}f)(\xi)=q^{-1/2}G(X,\psi_\xi)$. Thus $\alpha^{\#}$ affords a means of generalizing the Gaussian sum to X.

We will identify α with its matrix with respect to the standard basis for X, and $\alpha^{\#}$ with its matrix (a_{ij}) with respect to the basis $\{\psi_i\}$ of $L(X)$, where $\psi_i=\psi_{\xi_i}$ and $\xi_i\in X$.

THEOREM 1.4. $a_{ij}=q^{-n/2}\psi(\alpha^{-1}\xi_i\cdot\xi_j)$.

Proof. For $f=\sum_j b_j\psi_j\in L(X)$,

$$\alpha^{\#}f(\xi)=\sum_i\sum_j a_{ij}b_j\psi_i(\xi)=q^{-n/2}\sum_x f(x)\psi_\xi(\alpha x)$$

$$=q^{-n/2}\sum_x\sum_k b_k\psi_k(x)\psi_\xi(\alpha x).$$

Now let $f = \psi_j$ for a fixed ξ_j, so $b_k = \delta_{jk}$, and

$$\sum_i a_{ij}\psi_i(\xi) = q^{-n/2}\sum_x \psi_j(x)\psi_\xi(\alpha x)$$

$$= q^{-n/2}\sum_x \psi(x\cdot\xi_j)\psi_{\alpha x}(\xi)$$

$$= \sum_x q^{-n/2}\psi(\alpha^{-1}y\cdot\xi_j)\psi_y(\xi),$$

where

$$y = \alpha x.$$

Hence $a_{ij} = q^{-n/2}\psi(\alpha^{-1}\xi_i\cdot\xi_j)$. ∎

PROPOSITION 1.5. *$\alpha^\#$ is a unitary transformation.*

Proof. By Proposition 1.2 and Theorem 1.4, $(\alpha^\#)(\overline{{}^t\alpha^\#}) = I$.

2. THE EIGENVALUES OF $I_n^\#$

To understand how properties of α determine the properties of $\alpha^\#$, it is useful to first consider the transformation $I_n^\#$, where I_n is the identity transformation of X. Now

$$(I_n^\#)_{ij}^2 = q^{-n}\sum_k \psi(\xi_i\cdot\xi_k)\psi(\xi_k\cdot\xi_j)$$

$$= q^{-n}\sum_k \psi_k(\xi_i+\xi_k) = \begin{cases} 0, & \xi_i+\xi_j \neq 0, \\ 1, & \xi_i+\xi_j = 0 \end{cases}.$$

With $\xi_1 = 0$ and $\xi_i = -\xi_{q-i+2}$ for $i \neq 1$, the matrix $(I_n^\#)^2$ has the form shown in Figure 1. (This generalizes a method of Schur; see [1, p. 351]. Note that in the case $n = 1$, Carlitz has generalized Schur's method in a slightly different manner in [3].)

The characteristic polynomial of $(I_n^\#)^2$ is [writing I_{q^n} for the identity transformation of $L(X)$]

$$P(t) = \det\left[(I_n^\#)^2 - tI_{q^n}\right] = -(t-1)^{(q^n+1)/2}(t+1)^{(q^n-1)/2}$$

$$\left(I_n^{\#}\right)^2 = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 1 & \cdots & 0 & 0 \end{bmatrix}$$

FIG. 1

so the eigenvalues of $I_n^{\#}$ are ± 1, $\pm i$. Let m_1, m_2, m_3, and m_4 be the multiplicities of 1, -1, i, and $-i$, respectively, as eigenvalues. To determine these multiplicities, we note that $m_1 - m_2 + (m_3 - m_4)i = \operatorname{tr} I_n^{\#}$, $m_1 + m_2 = (q^n + 1)/2$, and $m_3 + m_4 = (q^n - 1)/2$. By Theorem 1.4,

$$\begin{aligned} \operatorname{tr} I_n^{\#} &= q^{-n/2} \sum_{x \in X} \psi(x \cdot x) \\ &= q^{-n/2} \sum_{x_1, \ldots, x_n \in F_q} \psi\left(x_1^2 + \cdots + x_n^2\right) \\ &= q^{-n/2} \left[\sum_{x_1} \psi\left(x_1^2\right)\right] \cdot \cdots \cdot \left[\sum_{x_n} \psi\left(x_n^2\right)\right] \\ &= q^{-n/2} \left[G(\chi, \psi)\right]^n; \end{aligned}$$

here and from now on χ is the quadratic character of F_q. (The last equality follows from a well-known property of Gaussian sums.) The value of $G(\chi, \psi)$ in this case can be found using the Hasse-Davenport relation (see, e.g., [5, p. 162]). If, for example, $p \equiv 1 \pmod 4$, $s \equiv 3$ (4), and $n \equiv 3$ (4), then $q \equiv 1$ (4), say $q = 4m + 1$, and $G(\chi, \psi) = \sqrt{q}$, so $\operatorname{tr} I_n^{\#} = 1$ and $m_1 = m + 1$, $m_2 = m_3 = m_4 = m$. The multiplicities in all other cases are as follows:

Case 1: $n \equiv 0$ (4). $q^n = 4m + 1$; $m_1 = m + 1$, $m_2 = m_3 = m$.

Case 2: $n \equiv 1$ (4).

(a) $p \equiv 1$ (4), so $q^n = 4m + 1$.

(i) s odd: $m_1 = m + 1$, $m_2 = m_3 = m_4 = m$.

(ii) s even: $m_2 = m + 1$, $m_1 = m_3 = m_4 = m$.

(b) $p \equiv 3$ (4).

(i) $s \equiv 0$ (4), so $q^n = 4m + 1$: $m_2 = m + 1$, $m_1 = m_3 = m_4 = m$.

(ii) $s \equiv 1$ (4), so $q^n = 4m + 3$: $m_1 = m_2 = m_3 = m + 1$, $m_4 = m$.

(iii) $s \equiv 2$ (4): $m_1 = m + 1$, $m_2 = m_3 = m_4 = m$.

(iv) $s \equiv 3$ (4): $m_1 = m_2 = m_4 = m + 1$, $m_3 = m$.

Case 3: $n \equiv 2\ (4)$.

(a) $q \equiv 1\ (4)$: $m_1 = m+1,\ m_2 = m_3 = m_4 = m.$

(b) $q \equiv 3\ (4)$: $m_2 = m+1,\ m_1 = m_3 = m_4 = m.$

Case 4: $n \equiv 3\ (4)$.

(a) $p \equiv 1\ (4)$.

(i) s odd: $m_1 = m+1,\ m_2 = m_3 = m_4 = m.$

(ii) s even: $m_2 = m+1,\ m_1 = m_3 = m_4 = m.$

(b) $p \equiv 3\ (4)$.

(i) $s \equiv 0\ (4)$: $m_1 = m+1,\ m_2 = m_3 = m_4 = m.$

(ii) $s \equiv 1\ (4)$: $m_1 = m_2 = m_3 = m+1,\ m_4 = m.$

(iii) $s \equiv 2\ (4)$: $m_2 = m+1,\ m_1 = m_3 = m_4 = m.$

(iv) $s \equiv 3\ (4)$: $m_1 = m_2 = m_4 = m+1,\ m_3 = m.$

3. THE GENERAL CASE

For any nonsingular α, i.e. $\alpha \in \mathrm{GL}_n(F_q)$, let $\alpha^* = {}^t\alpha^{-1}$.

THEOREM 3.1. *For $\alpha \in GL_n(F_q)$, define the $q^n \times q^n$ matrix $P_\alpha = (p_{ij})$ over C by $p_{ij} = 1$ if $\xi_i = \alpha\xi_j$; $p_{ij} = 0$ otherwise. Then*

(i) $\alpha^\# = P_\alpha I_n^\#$,

(ii) $P_\beta P_\alpha = P_{\beta\alpha}$ *for* $\beta \in GL_n(F_q)$,

(iii) $I_n^\# P_\alpha = (\alpha^*)^\# = P_{\alpha^*} I_n^\#$,

(iv) $(P_\alpha)^{-1} = {}^t(P_\alpha) = P_{\alpha^{-1}}$,

(v) $\alpha^\# \beta^\# = P_{-\alpha\beta^*}$,

(vi) $({}^t\alpha)^\# = {}^t(\alpha^\#)$.

Proof. (i): $(P_\alpha I_n^\#)_{ij} = q^{-n/2}\psi(\alpha^{-1}\xi_i \cdot \xi_j)$.

(ii): $(P_\beta P_\alpha)_{ij} = 1$ if and only if $\xi_i = \beta\xi_k$ and $\xi_k = \xi_j$ for some k; that is, $\xi_i = \beta\alpha\xi_j$.

(iii):

$$\left(I_n^\# P_\alpha\right)_{ij} = q^{-n/2}\psi\left(\xi_i \cdot \alpha\xi_j\right) = q^{-n/2}\psi\left({}^t\alpha\xi_i \cdot \xi_j\right)$$

$$= \left((\alpha^*)^\#\right)_{ij}.$$

(iv): $[P_\alpha {}^t(P_\alpha)]_{ij} = \delta_{ij}$.

(v):

$$\begin{aligned}\alpha^{\#}\beta^{\#} &= P_{\alpha}I_n^{\#}P_{\beta}I_n^{\#} \qquad \text{by (i)}\\ &= P_{\alpha}P_{\beta^*}\left(I_n^{\#}\right)^2 \qquad \text{by (iii)}\\ &= P_{\alpha}P_{\beta^*}P_{-I} \qquad \text{(see Section 2)}\\ &= P_{-\alpha\beta^*} \qquad \text{by (ii)}.\end{aligned}$$

(vi):

$$\begin{aligned}{}^t(\alpha^{\#}) &= {}^t\left(P_{\alpha}I_n^{\#}\right)\\ &= I_n^{\#}P_{\alpha^{-1}} \qquad \text{by (iv)}\\ &= P_{(\alpha^{-1})^*}I_n^{\#} \qquad \text{by (ii)}\\ &= ({}^t\alpha)^{\#}.\end{aligned}$$

■

In particular, if α is symmetric, then $\alpha^{\#}$ is symmetric and unitary; from (v) we see that in this case, $(\alpha^{\#})^2 = P_{-I}$, so $(\alpha^{\#})^4 = I_{q^n}$ and the eigenvalues of $\alpha^{\#}$ are ± 1, $\pm i$. If α is skew-symmetric, then $\alpha^{\#}$ is Hermitian and unitary $[({}^t\alpha)^{\#} = (-\alpha)^{\#} = \overline{(\alpha^{\#})} = {}^t(\alpha^{\#})]$; in this case $(\alpha^{\#})^2 = P_I = I_{q^n}$, so the eigenvalues of $\alpha^{\#}$ are ± 1.

COROLLARY 3.2. *Suppose that α and β are nonsingular and congruent; that is, there is a nonsingular γ such that $\beta = \gamma\alpha{}^t\gamma$. Then $\alpha^{\#}$ is similar to $\beta^{\#}$.*

Proof.

$$\begin{aligned}\beta^{\#} &= P_{\gamma}P_{\alpha}P_{{}^t\gamma}I_n^{\#} \qquad \text{by (ii)}\\ &= P_{\gamma}P_{\alpha}I_n^{\#}P_{\gamma^{-1}} \qquad \text{by (iii)}\\ &= P_{\gamma}\alpha^{\#}\left(P_{\gamma}\right)^{-1} \qquad \text{by (iv)}.\end{aligned}$$

■

COROLLARY 3.3. *The eigenvalues of $\alpha^{\#}$ are $2k$th roots of unity if $(-\alpha\alpha^*)^k = I_n$. Since $GL_n(F_q)$ is a finite group, such a k always exists.*

Proof. $(\alpha^{\#})^2 = P_{\alpha\alpha^*}(I_n)^2 = P_{-\alpha\alpha^*}$, so

$$(\alpha^{\#})^{2k} = P_{(-\alpha\alpha^*)^k} = P_I = I_{q^n}. \qquad \blacksquare$$

Next, we apply these results to the determination of the eigenvalues of $\alpha^{\#}$.

(i) First, assume α is a diagonal matrix with entries $\gamma_1, \ldots, \gamma_n$ on the main diagonal. Then

$$\begin{aligned}
\operatorname{tr}\alpha^{\#} &= q^{-n/2} \sum_{x \in X} \psi\left(\frac{1}{\gamma_1}x_1^2 + \cdots + \frac{1}{\gamma_n}x_n^2\right) \\
&= q^{-n/2} \prod_{i=1}^{n} G(\chi, \psi_{1/\gamma_i}) \\
&= \operatorname{tr} I_n^{\#} \prod_i \chi\left(\frac{1}{\gamma_i}\right) \quad \text{(by another property of Gaussian sums)} \\
&= \operatorname{tr} I_n^{\#} \prod_i \chi(\gamma_i).
\end{aligned}$$

Since α is symmetric, the eigenvalues of $\alpha^{\#}$ are ± 1, $\pm i$, and their multiplicities can be computed as in the case $\alpha = I_n$.

(ii) If α is symmetric, then α is congruent to a nonsingular diagonal matrix β. By Corollary 3.2, the eigenvalues of $\alpha^{\#}$ are the same as those of $\beta^{\#}$, which can be computed as above.

(iii) In the general case $\alpha \in \mathrm{GL}_n(F_q)$ we calculate the eigenvalues of $\alpha^{\#}$ by determining its characteristic polynomial $P(t) = C_0 t^{q^n} + C_1 t^{q^n - 1} + \cdots + C_{q^n}$, using a recursion formula from multilinear algebra:

$$C_r = -\frac{1}{r} \sum_{k=0}^{r-1} C_k \operatorname{tr}(\alpha^{\#})^{r-k} \qquad [4, \text{p. } 167].$$

Thus it is necessary to find $\operatorname{tr}(\alpha^{\#})^{\nu}$ for $1 \leqslant \nu \leqslant q^n$. For the case $\nu = 1$, we use

$$\begin{aligned}
\operatorname{tr}\alpha^{\#} &= q^{-n/2} \sum_{x \in X} \psi(\alpha^{-1}x \cdot x) \\
&= q^{-n/2} \sum_{x} \psi\left(\frac{1}{2}(\alpha^{-1} + \alpha^*)x \cdot x\right).
\end{aligned}$$

Now $\frac{1}{2}(\alpha^{-1} + \alpha^*)$ may be singular, but it is still congruent to a diagonal

matrix β, with entries $b_1,\dots,b_m,0,\dots,0$ on the main diagonal, where $b_i \neq 0$ if $1 \leqslant i \leqslant_m$. We find

$$\operatorname{tr}\alpha^{\#} = q^{-n/2} \sum_{x_1,\dots,x_m} \psi_{b_1}(x_1^2)\cdots\psi_{b_m}(x_m^2) q^{n-m}$$

$$= q^{n/2-m}[G(\chi,\psi)]^m \prod_{i=1}^{m} \chi(b_i).$$

For the case $\nu > 1$, we have

THEOREM 3.4. *If ν is even, then*

$$\operatorname{tr}(\alpha^{\#})^{\nu} = q^{\dim\ker[I_n - (-\alpha\alpha^*)^{\nu/2}]}.$$

If ν is odd, then $\operatorname{tr}(\alpha^{\#})^{\nu} = \operatorname{tr}([\alpha(-\alpha^*)^{(\nu-1)/2}]^{\#})$.

Proof.

$$\operatorname{tr}(\alpha^{\#})^{\nu} = q^{-\nu n/2} \sum_{\xi_1,\dots,\xi_\nu} \psi(\alpha^{-1}\xi_\nu\cdot\xi_1)\psi(\alpha^{-1}\xi_1\cdot\xi_2)\cdot\cdots\cdot\psi(\alpha^{-1}\xi_{\nu-1}\cdot\xi_\nu)$$

$$= q^{-\nu n/2} \sum_{\xi_1,\dots,\xi_{\nu-1}} \psi(\alpha^{-1}\xi_1\cdot\xi_2)\cdot\cdots\cdot\psi(\alpha^{-1}\xi_{\nu-2}\cdot\xi_{\nu-1})\cdot S$$

where $S = \sum_{\xi_\nu}\psi_\nu(\alpha^*\xi_1 + \alpha^{-1}\xi_{\nu-1})$. If $\xi_{\nu-1} = -\alpha\alpha^*\xi_1$ then $S = q^n$; otherwise $S = 0$. So

$$\operatorname{tr}(\alpha^{\#})^{\nu} = q^{-\nu n/2+n} \sum_{\xi_1,\dots,\xi_{\nu-3}} \psi(\alpha^{-1}\xi_1\cdot\xi_2)\cdot\cdots\cdot\psi(\alpha^{-1}\xi_{\nu-4}\cdot\xi_{\nu-3})\cdot S_1,$$

where $S_1 = q^n$ if $\xi_{\nu-3} = (-\alpha\alpha^*)^2\xi_1$ and $S_1 = 0$ otherwise. Continuing in this manner, we find that for ν even,

$$\operatorname{tr}(\alpha^{\#})^{\nu} = q^{-n} \sum_{\xi_1,\xi_2} \psi_{\xi_2}(\alpha^{-1}\xi_1 - \alpha^*(-\alpha\alpha^*)^{\nu/2-1}\xi_1)$$

$$= q^{\dim\ker[\alpha^{-1}+\alpha^*(-\alpha\alpha^*)^{\nu/2-1}]}$$

$$= q^{\dim\ker[I_n-(-\alpha\alpha^*)^{\nu/2}]}.$$

For ν odd,

$$\operatorname{tr}(\alpha^{\#})^{\nu} = q^{-n/2}\sum_{\xi_1}\psi\left(\alpha^{-1}\xi_1\cdot(-\alpha\alpha^*)^{(\nu-1)/2}\xi_1\right)$$

$$= \operatorname{tr}\left(\left[\alpha^*(-\alpha\alpha^*)^{(\nu-1)/2}\right]^{-1}\right)^{\#}.$$

Now

$$\left[\alpha^*(-\alpha\alpha^*)^{(\nu-1)/2}\right]^{-1} = \left[(-\alpha\alpha^*)^{-1}\right]^{(\nu-1)/2}\cdot {}^t\alpha$$

$$= (-\alpha {}^t\alpha^{-1})^{(\nu-1)/2}\cdot {}^t\alpha.$$

Since $({}^t\beta)^{\#} = {}^t(\beta^*)$ by Theorem 3.1(vi), we have

$${}^t\left[(-\alpha {}^t\alpha^{-1})^{(\nu-1)/2}\cdot {}^t\alpha\right]^{\#} = \left[\alpha(-\alpha {}^t\alpha)^{(\nu-1)/2}\right]^{\#};$$

since $\operatorname{tr} M = \operatorname{tr} {}^tM$, we find $\operatorname{tr}(\alpha^{\#})^{\nu} = \operatorname{tr}([\alpha(-\alpha^*\alpha)^{(\nu-1)/2}]^{\#})$. ∎

Thus the matrix calculations can become quite involved. Their extent depends upon the order of $-\alpha\alpha^*$ in the group $\mathrm{GL}_n(F_q)$.

4. TWO EXAMPLES

In our first example, the eigenvalues of $\alpha^{\#}$ turn out to be sixth roots of unity. In our second example, the eigenvalues of $\alpha^{\#}$ are fourth roots of unity although α is not symmetric; however, their multiplicities are different from any symmetric case.

EXAMPLE 4.1. If

$$q = p = 5 \quad \text{and} \quad \alpha = \begin{bmatrix} 1 & 2 \\ 0 & 4 \end{bmatrix},$$

then

$$\alpha = \alpha^{-1} \quad \text{and} \quad -\alpha\alpha^* = \begin{bmatrix} 0 & 2 \\ 2 & 4 \end{bmatrix}.$$

$(-\alpha\alpha^*)^3 = I_2$, so the eigenvalues of $\alpha^{\#}$ are sixth roots of unity. To find $\operatorname{tr}\alpha^{\#}$,

we use

$$\tfrac{1}{2}(\alpha^{-1}+\alpha^*)=\begin{bmatrix}1 & 1\\ 1 & 4\end{bmatrix},$$

which is congruent to $\begin{bmatrix}1 & 0\\ 0 & 3\end{bmatrix}$. So

$$\operatorname{tr}\alpha^{\#}=\tfrac{1}{5}[G(\chi,\psi)]^2\chi(1)\chi(3)=-1,$$

$$\operatorname{tr}(\alpha^{\#})^2=q^{\dim\ker(I_2-\alpha\alpha^*)}=1,$$

$$\operatorname{tr}(\alpha^{\#})^3=\operatorname{tr}\big([-\alpha\alpha^*\alpha]^{\#}\big)=5,$$

which is found using the method of the $\nu=1$ case. Similarly, we find $\operatorname{tr}(\alpha^{\#})^4=1$ and $\operatorname{tr}(\alpha^{\#})^5=-1$. Because $(\alpha^{\#})^6=I_{25}$, we have $\operatorname{tr}(\alpha^{\#})^6=25$; for $\nu>6$, $\operatorname{tr}(\alpha^{\#})^{\nu}=\operatorname{tr}(\alpha^{\#})^{\nu \bmod 6}$. Using the formula for the coefficients of $P(t)$, we get $C_1=-(-\operatorname{tr}\alpha^{\#})=-1$, $C_2=-\tfrac{1}{2}[-\operatorname{tr}(\alpha^{\#})^2+C_1\operatorname{tr}\alpha^{\#}]=0$, $C_3=-\tfrac{1}{3}[-\operatorname{tr}(\alpha^{\#})^3+C_1\operatorname{tr}(\alpha^{\#})^2+C_2\operatorname{tr}\alpha^{\#}]=2$, etc. Continuing, we find

$$\begin{aligned}P(t)&=-[t^{25}+t^{24}-2t^{22}-2t^{21}-2t^{19}-2t^{18}+6t^{16}\\ &\qquad+6t^{15}-6t^{10}-6t^9+2t^7+2t^6+2t^4+2t^3-t-1]\\ &=-(t^6-1)^3(t^3-1)^2(t+1).\end{aligned}$$

If we write $\varepsilon=e^{\pi i/3}$, then the eigenvalues ε and ε^5 have multiplicity 3, ε^2 and ε^4 have multiplicity 5, 1 has multiplicity 5, and -1 has multiplicity 4.

EXAMPLE 4.2. Here $q=p=3$ and $n=3$. See Figure 2: $(-\alpha\alpha^*)^2=I_3$, so the eigenvalues of $\alpha^{\#}$ are fourth roots of unity. Now $\operatorname{tr}\alpha^{\#}=3i$, $\operatorname{tr}(\alpha^{\#})^2=9$,

$$\alpha=\begin{bmatrix}1 & 2 & 1\\ 2 & 1 & 1\\ 1 & 0 & 1\end{bmatrix}\qquad \alpha^{-1}=\begin{bmatrix}1 & 1 & 1\\ 2 & 0 & 1\\ 2 & 2 & 0\end{bmatrix}$$

$$\alpha^*=\begin{bmatrix}1 & 2 & 2\\ 1 & 0 & 2\\ 1 & 1 & 0\end{bmatrix}\qquad -\alpha\alpha^*=\begin{bmatrix}2 & 0 & 0\\ 2 & 1 & 0\\ 1 & 0 & 1\end{bmatrix}$$

FIG. 2

and $\mathrm{tr}(\alpha^{\#})^3 = -3i$ (computed as above); also $\mathrm{tr}(\alpha^{\#})^4 = 27$, $\mathrm{tr}(\alpha^{\#})^5 = \mathrm{tr}\,\alpha^{\#}$, etc. Next, we apply the recursion formula and find $C_1 = 3i$, $C_2 = 9$, $C_3 = 19i$, and so on. the characteristic polynomial of $\alpha^{\#}$ is $-(t^2-1)^9(t-i)^6(t+i)^3$; using m_1, m_2, m_3, and m_4 as in Section 2, we have $m_1 = m_2 = 9$, $m_3 = 6$, and $m_4 = 3$.

REMARK

These results are included in the author's doctoral dissertation [2].

The author wishes to thank the referee for several helpful comments.

REFERENCES

1 Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic, New York, 1966.
2 P. S. Bremser, Some studies on character sums over finite fields, Ph.D. Thesis, Johns Hopkins Univ., Baltimore, 1984.
3 L. Carlitz, Some cyctolomic matrices, *Acta Arithmetica* 5:293–308 (1959).
4 W. H. Greub, *Multilinear Algebra*, Springer, New York, 1967.
5 H. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York, 1982.
6 R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesely, Reading, Mass., 1983.